

## SV: Honeypot detection and countermeasures

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-06/0120.html>

---

**From:** Trygve Aasheim ([trygve.aasheim\\_at\\_bbs.no](mailto:trygve.aasheim_at_bbs.no))

**Date:** 06/24/03

Date: Tue, 24 Jun 2003 13:48:49 +0200

To: "Rob Shein" <[shoten@starpower.net](mailto:shoten@starpower.net)>, "Michael Boman" <[michael.boman@securecirt.com](mailto:michael.boman@securecirt.com)>, "Larry Co

exactly.

And another point is that it's very easy to understand that a machine is a honeypot. Usually, they are sitting ducks. If the pen-test guys manage to use an exposed resource to try to get further in, they won't see the honeypots unless they scan the net. And a scan is not something you really want to do...(it will give you away, and a company that hires a pen-test crew probably has some IDS systems). If the pentest guys just run netstat, to check what internal IPs are connected to the host they are using, then they have the info they need.

When sniffing the traffic, over time, you will see what goes between different machines, and the honeypots won't be included in this "production traffic", or in any netstat tables.

The sniffer will over time reveal the machines though (due to different \*cast traffic)...but since they won't be included in the general traffic on the net, they won't be of interest to a person wanting to break in, or a pen-test crew. Atleast if they got some skills...

The more unskilled ones might fire up nmap and do a flat scan, revealing the hosts...and trying to break into them...but is it really those tools you want a signature of?

Probably not...since you should be protected by those type of people in your standard security setup...

Another thing is...if you want to "steal" the other companies "tools"...how are you going to do that by just looking at the traffic? What's interesting is not the packets going back and forth...but the tools in the other end, analyzing the data it gets from those packets.

But...the last thing, since that was commented (but was removed from the thread I'm answering on). If you hire a company to do a pentest, of course you don't tell them about your countermeasures. The pentest is the exam for the system you have deployed, and the guys that tests you are the examiners. The result from the pentest should/might include that, yes, they found the honeypots, and it distracted them for some time before they understood what they had hit (a honeypot is just another countermeasure), and then the rest of the report comes.

If you want to pentest a new service, then of course point them at that service. If you want to pentest your company...then that's what you tell them.

Regards,  
Trygve Aasheim

## SecurityFocus Penetration: SV: Honeypot detection and countermeasures

Manager, Network Security

-----Opprinnelig melding-----

Fra: Rob Shein [mailto:shoten@starpower.net]

Sendt: 23. juni 2003 15:58

Til: 'Michael Boman'; 'Larry Colen'

Kopi: 'Brass, Phil (ISS Atlanta)'; pen-test@securityfocus.com

Emne: RE: Honeypot detection and countermeasures

This wouldn't work. Seeing the packets/traffic on the wire doesn't tell you the tools that are used, and it also doesn't really give you much else. Considering that a honeypot is either not really rootable (DTK) or is very low hanging fruit (and very rootable, like a honeynet.org system), they either won't see tools downloaded to the system or won't see anything more than the bare minimum needed to exploit a system that is too vulnerable to begin with.

> -----Original Message-----

> From: Michael Boman [mailto:michael.boman@securecirt.com]

> Sent: Wednesday, June 18, 2003 11:32 PM

> To: Larry Colen

> Cc: Brass, Phil (ISS Atlanta); pen-test@securityfocus.com

> Subject: Re: Honeypot detection and countermeasures

>

>

> On Wed, 2003-06-18 at 10:15, Larry Colen wrote:

>> Good point. I was more envisioning a scenario where the client was

>> testing the whole security system, including the honeypots. I.e.

>> hiring a pen-tester without giving the pen-tester any

> knowldege of the

>> system before hand.

>>

>> If I seem like a clueless newbie, I hope that I at least

> seem like a

>> polite clueless newbie. I'll crawl back into my hole and lurk a bit

>> more.

>>

>> Larry

>>

>

> There is a viable scenario for this. Let's say ACME Inc.

> wants to do their own pen-tests because they

> - Don't like to pay outsiders to do it

> - Want to compete with the company

> - They want to steal their tools and techniques

> - insert your own paranoid explanation for the "why" bit

>

> They hire a group of people to hack their systems and record

> everything so once the exercise is over ACME Inc. now knows

> the tools and techniques of that particular pen test group.

>

SV: Honeypot detection and countermeasures

## SecurityFocus Penetration: SV: Honeypot detection and countermeasures

> *It's unlikely, but possible. Haven't happen to me (yet).*  
>  
> *Best regards*  
> *Michael Boman*  
>  
> --  
> *Michael Boman*  
> *Security Architect, SecureCiRT Pte Ltd <http://www.securecirt.com>*  
>

---

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team? Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Visit us at: [www.coresecurity.com/promos/sf\\_ept1](http://www.coresecurity.com/promos/sf_ept1)  
or call 617-399-6980

---

---

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team? Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Visit us at: [www.coresecurity.com/promos/sf\\_ept1](http://www.coresecurity.com/promos/sf_ept1)  
or call 617-399-6980

---